(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 February 2005 (24.02.2005)

PCT

(10) International Publication Number
WO 2005/018138 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number: PCT/US2003/024000

(22) International Filing Date: 31 July 2003 (31.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: THOMSON LICENSING S.A. [FR/FR]; 46, Quai A. Le Gallo, F-92648 Boulogne (FR).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: RHOADS, Steven, Charles [US/US]; 140 Parkview Road, Carmel, IN 46032 (US).

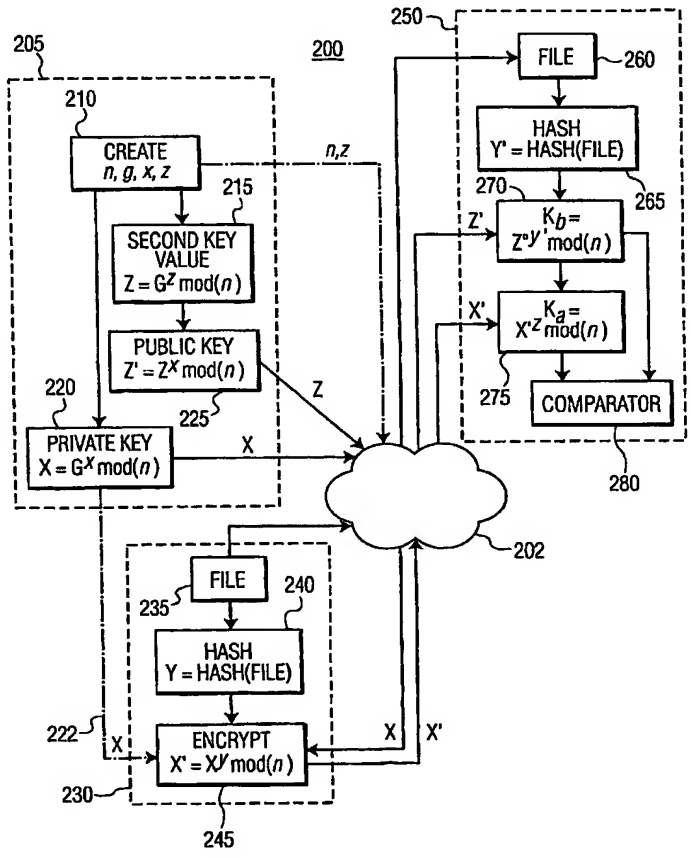
(74) Agents: TRIPOLI, Joseph, S. et al.; c/o Thomson Licensing Inc., Suite #200, Two Independence Way, Princeton, NJ 08540 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: GENERATION AND VALIDATION OF DIFFIE-HELLMAN DIGITAL SIGNATURES



(57) Abstract: In one embodiment, a device for decoding digital signatures to validate the source of received information items is disclosed. The device is operable to determine a first comparator value in relation to a first value associated with information items received over a network and a Diffie-Hellman public key, determine a second comparator value in relation to a digital signature received, wherein the digital signature is determined in association with a second value associated with the information items prior to transmission over said network, and comparing the first and second comparator values to validate the source based on the comparison. In another embodiment, a key generating device is operable to generate a first and second Diffie-Hellman key from a plurality of large numbers randomly selected, wherein at least one of the numbers is a prime number, and further determine a public key as a Diffie-Hellman transpose of one of the generated first and second Diffie-Hellman keys.

WO 2005/018138 A1

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.